REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-05-2013	FINAL	

4. TITLE AND SUBTITLE

Cyber Power and Operational Art:
A comparative analysis with air power

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Bradley D. Converse, LCDR, USN

Paper Advisor: Prof Paul Povlock

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The rapid advance in computer technology over the past few decades – and even years – has far out-paced military cyber operations doctrine. This is not unlike the interwar period between the First and Second World Wars when aircraft technology was undergoing a rapid acceleration of capabilities, leaving theorists to postulate about the best integration of this new technology into military operations. This paper analyzes early air power theory in comparison to the burgeoning cyber power debate, and concludes that aside from strategic defense, U.S. military cyber power should be focused at the operational level of war. Using the lessons and framework provided by the evolution of air power, operational level offensive and defensive cyber operations must be incorporated into a combined arms approach with other joint force capabilities. Focusing on the appropriate level of war and reorganizing existing joint task force command structures will help ensure synergy throughout the warfighting domains, resulting in a more integrated, synchronized, and effective joint force.

15. SUBJECT TERMS

Cyberspace, cyber power, cyber doctrine, cyber warfare, cyberspace operations, CYBERCOM, airpower, interwar airpower theory

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Chairman, JMO Dept
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		23	401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

CYBER POWER AND OPERATIONAL ART: A comparative analysis with air power

by

Bradley D. Converse

LCDR USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

20 May 2013

Contents Page

Paper Abstract

Cyber Power and Operational Art: A comparative analysis with air power

The rapid advance in computer technology over the past few decades – and even years – has far out-paced military cyber operations doctrine. This is not unlike the interwar period between the First and Second World Wars when aircraft technology was undergoing a rapid acceleration of capabilities, leaving theorists to postulate about the best integration of this new technology into military operations – air power. This paper analyzes early air power theory in comparison to the burgeoning cyber power debate, and concludes that aside from strategic defense, U.S. military cyber power should be focused at the operational level of war. Using the lessons and framework provided by the evolution of air power, operational level offensive and defensive cyber operations must be incorporated into a combined arms approach with other joint force capabilities. Focusing on the appropriate level of war and reorganizing existing joint task force command structures will help ensure synergy throughout the warfighting domains, resulting in a more integrated, synchronized, and effective joint force.

INTRODUCTION

> *Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.*
>
> - Italian Air Marshall Giulio Douhet (1928)

Just a few decades ago, millions of transistors or thousands of vacuum tubes powered massive, stand-alone computers. Now, microprocessors run pocket-sized personal electronic devices that transmit and receive data at speeds previously unimaginable. This rapid advance in computer technology and information sharing has left practitioners of military cyber operations gasping to maintain doctrinal relevance. The existing doctrine generally resulted from this new burgeoning technology and not vice versa. As evidence, the term "cyberspace" has existed for over 30 years, yet versions of joint U.S. military cyber operations doctrine have only recently begun to emerge.[1] This situation is not unlike the interwar period between the First and Second World Wars when aviation technology was undergoing a rapid acceleration of capabilities. During this time, military theorists attempted to convey their thoughts on the most effective translation of this new technology into military capability and practice, which they referred to as air power. Giulio Douhet, B. H. Liddell Hart, Billy Mitchell, Hugh Trenchard, Alexander P. de Seversky, and myriad others, all argued in their own ways that air power could achieve independent, strategically decisive effects. With the benefit of hindsight (and good intentions aside), these theorists were perhaps better evangelists than soothsayers.

[1] There remains no universally accepted definition of cyberspace. Some common definitions refer to cyberspace as a notional environment in which communication over computer networks occur – the "online world." In contrast, U.S. military joint doctrine defines cyberspace as "a global domain consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13 Information Operations* (Washington D.C.: U.S. Department of Defense, 2012), II-9.

Much the same can be said of today's cyberspace and military cyber power debate.[2] It is not feasible to believe that cyberspace operations alone can achieve independent, strategically decisive effects.[3] Again, an eerily similar debate occurred in the past. The technology and medium of air and cyber may be different, but sufficient parallels exist for important lessons to apply. Thus, not unlike the unrealized assertions of the air power advocates during the interwar years, cyberspace operations will prove strategically disappointing, but will be decisive at the operational level of war if incorporated into a combined arms approach with existing military capabilities.

Many current advocates of cyber power tend to ignore the operational level of war, and instead focus on the potential strategic capability of cyber weapons used to mount so-called cyber attacks.[4] In doing so, they reveal some of the same flawed assertions of air power proponents prior to the Second World War who believed that the very character of warfare had changed forever with the invention of flying machines, and the strategic impact air power was destined to have on the next war. While one can argue that air power indeed changed the character of warfare, it fell well short of achieving the decisive strategic results Douhet and his contemporaries had predicted. However, air power did revolutionize warfare and to this day remains decisive when correctly employed by operational commanders and

[2] Military cyber power refers to the ability to conduct cyber operations in and from cyberspace. John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quartlery* (Summer 2011): 96.

[3] U.S. joint doctrine defines cyberspace (or cyber) operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-12 Cyberspace Operations* (U) (Washington D.C.: U.S. Department of Defense, 2013), II-1 (Secret Rel USA/FVEY). Information extracted is unclassified.

[4] There are many types of cyber weapons that can be used to conduct a cyber attack. This paper is limited to discussion of those weapons that are employed in or through cyberspace, not weapons from outside cyberspace that target physical aspects of the cyber domain (e.g. a directed energy weapon aimed at crippling a computer server "farm"). In this context, some common examples of cyber weapons are the botnet, virus, worm, and Trojan horse that can be used to execute various types of distributed denial-of-service and/or malicious software cyber attacks. Derek S. Reveron, ed., *Cyberspace and national security: threats, opportunities, and power in a virtual world* (Washington D.C.: Georgetown University Press, 2012), 8.

planners. What does this mean for cyber power theories and cyber operations doctrine moving forward toward what could be the next conflict? Conclusions based on the comparative evidence will provide implications for policy makers, military leaders, and students of operational art.

COUNTERARGUMENT (Cyber Power as Strategically Decisive)

> *And cyber is now at a point where the technology is there to cripple a country, to take down our power grid system, to take down our government system, take down our financial system and literally paralyze the country.*
>
> - Former Secretary of Defense Leon Panetta (2013)

A strategic objective is "one whose destruction, annihilation, neutralization, or control will have a drastic (or radical) effect on the course and outcome of a war as a whole."[5] Furthermore, U.S. Joint Doctrine refers to a strategic attack as one aimed at weakening an enemy's ability or will to continue to engage in conflict or action.[6] Former Secretary of Defense Panetta's quote above may well describe the essence of a strategic attack aimed at achieving strategic objectives with corresponding effects. It is apparent and appropriate that U.S. leaders are concerned about the cyber threat. However, while the need to develop cyber defense against such a threat may be evident, other leaders are persistently pressing to pursue offensive cyber capabilities aimed at strategically affecting possible adversaries.

Senator Jim Inhofe (R-Oklahoma), Ranking Member of the U.S. Armed Services Committee, stated in March 2013 that the "relatively low cost potential of offensive cyber

[5] Milan Vego, *Joint Operational Warfare: Theory and Practice* (2007; repr., Newport, RI: U.S. Naval War College, 2009), II-3.
[6] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0 Joint Operations* (Washington D.C.: U.S. Department of Defense, 2011), III-26.

must be a priority" for the Department of Defense (DOD).[7] He also asserts that power projection in the cyber domain is part of the "full spectrum of strategic capabilities [that] must not be overlooked, as they are the nation's ultimate insurance policy."[8] There is also no shortage of cyber power advocates who postulate that the potential effects of a cyber attack warrant an emphasis on offensive cyber operations aimed at achieving significant strategic results. References to actions taken in cyberspace "exploding fuel refineries, frying power grids or blinding air traffic controllers," or to a potential "cyber-Pearl Harbor," emphasize the need to prepare for the coming cyberwar – a war that will be fought and won through no means or domain other than strategic cyber weapons and cyberspace.[9]

Proponents of cyber power argue that the new domain of cyberspace (added to the existing domains of land, sea, air, and space) has brought about "the birth of a new era of human conflict."[10] To many, cyber power is "unique and ubiquitous" in that it can generate absolute and simultaneous strategic effects in all domains.[11] Invoking Sun Tzu, cyber theorists often claim that cyber warfare epitomizes what Master Sun called the "supreme excellence" of war fighting, which is to fight without fighting and to achieve victory without spilling blood.[12]

Historian and strategist Gregory Copley, president of the International Strategic Studies Association, believes this new era represents a post-Cold War transition from the

[7] James M. Inhofe, "Inhofe Opening Statement at Oversight Hearing for STRATCOM, CYBERCOM," The Office of Senator James N. Inhofe, March 13, 2013, http://www.inhofe.senate.gov/newsroom/press-releases/-inhofe-opening-statement-at-oversight-hearing-for-stratcom-cybercom.
[8] Ibid.
[9] *The Economist*, "Cyber-warfare: Hype and Fear," December 8, 2012, http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may
[10] Richard Stiennon, *Surviving Cyberwar* (Lanham, MD: Government Institutes, 2010), 1.
[11] Reveron, *Cyberspace and national security*, 210.
[12] Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2010), 2.

nuclear age to the cyber age.[13] Specifically, he asserts that offensive cyber warfare can be precisely employed and accomplish comprehensive strategic effects, even surpassing the effects that nuclear weapons can achieve.[14] Accordingly, Copley claims "nuclear weapons have already been eclipsed by cyber weapons, just as all weapons are ultimately tamed by others."[15] This notion seems to be based on the belief that 21st century society has become so technologically dependent that cyber weapons are now capable of inflicting mass destruction that "can achieve widespread population chaos or panic [that] has traditionally led to the collapse of states and empires."[16] Challenging Mother Nature, Copley asserts, "Major natural disasters are but kisses on the cheek of society compared with the potential impact of unrestricted cyber warfare."[17]

Copley is certainly neither alone as a fervent cyber proponent who promotes the use of offensive cyber capabilities at the strategic level of war, nor is he the first. For instance, Chinese People's Liberation Army Colonels Qiao and Wang emphasize cyber war actions in their seminal work *Unrestricted Warfare,* a text about the future of war written in 1999. They claim, "One hacker + one modem causes an enemy damage and losses almost equal to those of war [and] because it has a breadth and secrecy of trans-level combat, this method of individual combat very easily achieves results on the strategic and even war policy levels."[18]

[13] Gregory Copley, "The Transition Beyond Strategic Nuclear War," (Defense and Foreign Affairs Strategic Policy 40 no. 11/12, 2012), 4.
[14] Gregory Copley, "P3R: Projection, Protection, Policing, Resilience," (Defense and Foreign Affairs Strategic Policy 40 no. 11/12, 2012), 2.
[15] Gregory Copley, "The Transition Beyond Strategic Nuclear War," 6.
[16] Gregory Copley, "P3R: Projection, Protection, Policing, Resilience," 18.
[17] Ibid., 19.
[18] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 199.

Military theorists from Russia also actively lobby for cyber doctrine that includes targeting an enemy's population in order to achieve strategic results.[19]

In terms of the U.S. military, the belief that offensive cyber operations (friendly or enemy) will likely yield strategic effects led the DOD to formally recognize U.S. Cyber Command (CYBERCOM) as a subordinate unified command under U.S. Strategic Command (STRATCOM) in 2009.[20] The placement of U.S. cyber forces under STRATCOM underscores the DOD's mindset of cyber operations being controlled at the strategic level of war. Recently, there has been the establishment of Cyber Support Elements (CSEs) apportioned to both geographic and functional combatant commands. However, CYBERCOM retains operational control of the CSEs, which serve mainly as a tool to coordinate and deconflict during the combatant commander's planning process. The CSEs are not the only cyber forces located at the combatant commands. Other cyber warriors have recently been organized into Joint Cyberspace Centers (JCCs) that provide at least some dedicated assets focused at the operational level of war – albeit insufficiently focused and resourced as of yet. [21]

DISCUSSION / ANALYSIS (Air Power's Strategic Disappointment as a Premonition)

> *The advent of air power, which can go straight to the vital centers and either neutralize or destroy them, has put a completely new complexion on the old system of making war. It is now realized that the hostile main army in the field is a false objective, and the real objectives are the vital centers.*
>
> - Brigadier General William "Billy" Mitchell (1930)

[19] Jeffrey Carr, *Inside Cyber Warfare*, 167.
[20] Richard M. Crowell, "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare," (Newport: Naval War College, 2012), 8.
[21] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-12* (U), II-1 (Secret Rel USA/FVEY). Information extracted is unclassified.

Cyber theorists who claim that the wars of the future will be bloodless and non-kinetic in nature, fought by cyber warriors wreaking havoc on opposing nations through cyberspace, need look no further than 80 years in the past to see similar prophecies proved wrong. The terrible trench warfare and awful attrition of the First World War was to be leapfrogged by technology and innovation, supposedly changing war itself through the strategic capabilities of air power. After WWII, and tens of millions of casualties later, the world was disappointed.

Offense the preferred form of air warfare

Giulio Douhet, a WWI combat veteran-turned interwar air power theorist, conjectured that air power was revolutionary because of the new domain in which it operated, not necessarily because of the weapons systems that were being developed.[22] The speed, range, and flexibility of aircraft would render useless offensive operations on land. Armies would now adopt a strictly defensive mindset while air forces pounded the enemy into submission through massive offensive operations designed to gain command of the air and destroy an enemy's strategic "vital centers."[23] It is important to remember that air defenses were in their infancy when Douhet published his treatise, *The Command of the Air*. Thus, he argued that the aerial offensive was preferred over defensive operations. Given the vastness of the air domain, defense seemed more than difficult; to him it was impossible.[24]

Interestingly, current cyber theorists make similar arguments about cyberspace where the offense currently dominates defenses because attacks can occur at great speed and range is not an issue. Furthermore, cyber attacks can occur from anywhere in the world, detection

[22] Philip S. Melinger, ed., *The Paths of Heaven: The Evolution of Airpower Theory* (Maxwell AFB, AL: Air University Press, 1997), 9.
[23] Ibid., 10.
[24] Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (Washington D.C.: Air Force History and Museums Program, 1998), 24.

is difficult, and cyber threat elimination is deemed even more difficult. These factors combine to put cyber defenses under great pressure.[25] However, perhaps cyber theorists are being presumptuous by ignoring a tenant of the great Prussian war theorist Carl von Clausewitz, who wrote that "the defensive form of warfare is intrinsically stronger than the offensive."[26]

Strategic focus to achieve or maintain independence

Aside from focusing on the offense over defense, another similarity between today's cyber debate and that of early air power is the concept of using offensive operations to target strategic transportation, population, and industrial centers (referred to in cyber parlance as "critical infrastructure"). Renowned strategist Sir Basil Liddell Hart reflected upon interwar air power theory in a lecture given at the U.S. Naval War College in 1952. He stated that air power "promised new scope for producing paralysis" of the enemy by affording the ability to fly over his main forces unopposed, striking military and civil centers in order to achieve "physical and moral effects."[27] In this vein, one of the most prolific air power advocates of his time, Alexander de Seversky, argued that victory could and would be achieved through the application of air power. The title of his most famous work, *Victory Through Air Power*, summarized this sentiment. Seversky fervently lobbied for air power to be used against mainly strategic industrial targets in order to cripple an enemy's war producing efforts.[28] Unlike Seversky who would claim after the war that air power had been the decisive factor in

[25] Fred Schreier, "On Cyberwarfare," Geneva Center for the Democratic Control of Armed Forces Horizon 2015 Working Paper Series (2012): 12, http://www.dcaf.ch/Publications/On-Cyberwarfare
[26] Carl von Clausewtiz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 358.
[27] Sir Basil Henry Liddell Hart, "The Objective in War: National Object and Military Aim," Naval War College Review V no. 4 (1952): 14.
[28] In terms of strategic targeting, Seversky disagreed with Douhet who believed the will of the civilian population was the key objective. John Gooch, ed., *Airpower: Theory and Practice* (Portland, OR: Frank Cass, 1995), 19.

victory, Liddell Hart instead believed that attacks on industrial centers did not have the predicted decisive effects and instead produced another "prolonged war of attrition . . . with perhaps less killing but more devastation than the 1914-18 form."[29]

The arguments for offense being preferred over defense and for focus on purely strategic effects most likely came about because air power proponents were attempting to influence the debate over an independent aviation force, especially in the United States. In order to make the changes necessary to wage "modern" war, the argument went, there needed to be an air force separate from the army. This would guarantee the ability to independently apply air power without being shackled with the responsibility to always support the army.[30] In order to "sell" an independent air force to the public and in turn the politicians, the air arm had to have a winning capability that would make it at least equal, if not superior, to the already existing services.[31] Thus, "the doctrine of victory through strategic bombing came first, the means to achieve it later."[32] One of the most outspoken supporters of achieving independence for what would later become the United States Air Force was Brigadier General William "Billy" Mitchell. Indeed, it seems that Mitchell actually led an insurgency of sorts against his army "rulers," claiming that air power would independently win the next war through a strategy of "obliteration based on calculation."[33]

While not clamoring for a separate military service, similar claims using cyber power instead of air power to achieve war-winning, strategic results certainly do not hurt the chances for CYBERCOM to receive its share of a now fiercely contested DOD budget. This

[29] Sir Basil Henry Liddell Hart, "The Objective in War," 22.
[30] Philip S. Melinger, *The Paths of Heaven*, 89.
[31] William O'Neill, *A Democracy at War: America's Fight at Home and Abroad in World War II* (New York: The Free Press, 1993), 302.
[32] Ibid.
[33] John Gooch, *Airpower*, 3.

is certainly not to say that claims about the vulnerabilities of U.S. networks are false. The threat is very real, and therefore should result in a disproportionally balanced focus on first reinforcing cyberspace network defenses and then developing limited offensive cyber capabilities.

Strategic disappointment versus operational success

With all of this in mind, the first incorporation of Western air power theories into war operations and tactics led to mixed strategic success at best. Perhaps it was an over-inflated sense of strategic ability that ironically harmed air power's evolution as a decisive instrument of war.[34] This was because the "overreach in claimed ability [led to] an immense underreach in claims for the benefits of . . . nonstrategic air power."[35] In other words, a narrow and exaggerated initial focus on air power as a strategic instrument overshadowed the operational and tactical level effects actually achieved. For commanders in the field, there was no doubt as to the ability of air power to exploit vulnerabilities and achieve operational success. For instance, General Erwin Rommel, after being defeated by the Allies in the battle for France in 1944 remarked, "Anyone who has to fight, even with the most modern weapons, against an enemy in complete command of the air, fights like a savage against modern European troops, under the same handicaps and with the same chance of success."[36]

Rommel was not alone in this observation. Post-WWII analysis of the European theater proved that air power had a "decisively crippling effect" on the German army and virtually assured victory.[37] This decisiveness was achieved mainly through the actions of the air forces against communications and transportation targets on mainland Europe, enabling

[34] Colin S. Gray, *Airpower for Strategic Effect* (Maxwell AFB, AL: Air University Press, 2012), 34.
[35] Ibid., 35.
[36] Davis Betz and Tim Stevens Cyberspace and the State (London, UK: International Institute for Strategic Studies, 2011), 88-89.
[37] Sir Basil Henry Liddell Hart, "The Objective in War," 18.

the Allied invasion of the continent.[38] For example, the bombing effects on German rail traffic were detrimental to the Wermacht's combat power build up and resupply efforts during the Normandy invasion.[39] As for the strategic effects from independently bombing the vital population and industrial centers, "the results fell far short of what was being claimed . . . by those who were conducting it."[40] This was because strategically affecting the citizenry's support of the war effort proved nearly futile and almost impossible to predict, even after the RAF Bomber Command's extensive worker "de-housing" campaign.[41] Likewise, U.S. air planners failed to comprehend the true industrial capacity of the Germans, grossly underestimating the German capability to substitute for destroyed materials and to produce weapons systems such as aircraft and tanks.[42] Thus, the two main strategic targets of the Allied bombing forces – popular support and industrial infrastructure – yielded disappointing results in terms of proving decisive in victory. Interestingly, the criticality of these two targets is mentioned in a vast majority of current cyber power debates.

Air power and operational art

Some nations during the interwar period did not subscribe to the theorized strategic decisiveness of air power leading up to WWII. The Russians (then Soviets) were one power who did not agree and instead prescribed to a combined arms approach with their air power assets aimed at achieving operational objectives. Perhaps this was because they had a much better understanding of operational art, being that the former tsarist general Aleksandr' A.

[38] Sir Basil Henry Liddell Hart, "The Objective in War," 18.
[39] William O'Neill, *A Democracy at War*, 313.
[40] Sir Basil Henry Liddell Hart, "The Objective in War," 19.
[41] The RAF's Bomber Command began to target German cities in early 1942. It was Prime Minister Churchill's science advisor who tactfully used "de-housing the workers" as a way of referring to "destroying German morale by destroying German citizens." William O'Neill, *A Democracy at War*, 306.
[42] Joseph F. Birchmeier, *The Reliability of Warden's Theory on the Use of Air Power* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2000), 11.

Svechin coined the term.[43] This understanding of operational art was described as the theory and practice of preparing and conducting military actions on land, sea, and in the air.[44] Consequently, they believed that "one of the most important tasks of aviation is active assistance to the ground and naval forces in all the forms of their combat activity."[45] The effectiveness of the Soviet approach could be seen in many areas, not the least of which was that three quarters of all German aircraft losses during WWII came at the hands of the Red Air Force fighting on the Eastern Front.[46]

Remarkably, U.S. forces did not use the term operational art until near the end of the Cold War. After appearing in different forms throughout various service and joint publications, current U.S. joint doctrine refers to operational art as "the use of creative thinking by commanders and staffs to design strategies, campaigns, and major operations and organize and employ military forces."[47] Put simply, it is a mindset not only desired, but required, of operational commanders and planners in order to achieve unified action toward an objective. The decision to independently employ air forces seeking almost exclusively strategic effects was detrimental to unified action and thus violated one of the precepts of warfare: unity of effort.[48] Especially in the European theater, "strategic bombing" diverted military and economic resources to build and employ an extensive heavy bomber fleet.[49]

---

[43] Milan Vego, *Joint Operational Warfare*, I-3.
[44] Ibid., I-5.
[45] Mark A. Admiral, *The Evolution of Russian Offensive Air Warfare Theory: From Deep Battle to Aerospace War* (Monterey, CA: Naval Postgraduate School, 1993), 33.
[46] Ibid., 43.
[47] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0*, II-3.
[48] U.S. joint doctrine defines unity of effort as the coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization. Ibid., A-2.
[49] Colin S. Gray, *Airpower for Strategic Effect*, 117.

These bomber aircraft often launched seeking attainment of objectives not well defined and sometimes at the detriment of other concurrent major operations – especially those on land.[50]

However, unity of effort was eventually achieved with improved integration of air power into operations. When air power was properly synchronized with actions in the other domains of sea and land (which at the time of WWII were the only other warfighting domains), its true potential as a decisive instrument came to light.[51] As was presented earlier, air power was decisive in enabling the invasion of the European continent and eventual Allied victory. This decisiveness was achieved because operational commanders properly directed and synchronized military operations, including air operations, toward a common goal.[52] Prior to 1944, the staffs of the Allied Air Forces were not as eager to conduct operations in pursuit of clearly defined military objectives as they were to "pursue independent operations against civil objectives – the attack on the industrial centers of the opposing country."[53] By opting for more unified action across the Allied land and air forces, the Allies were finally able to secure success.

CONCLUSIONS and RECOMMENDATIONS (Combined Arms in Doctrine)

> *Applying combat power depends on combined arms to achieve its full destructive, disruptive, informational, and constructive potential. Combined arms is the synchronized and simultaneous application of arms to achieve an effect greater than if each arm was used separately or sequentially.*
>
> - Army Doctrine Publication 3-0 (2011)

The parallels between the air power controversy of the interwar period and the current cyber power debate are clear and numerous. Although air power has perhaps never lived up

[50] William O'Neill, *A Democracy at War*, 315, 318.
[51] Colin S. Gray, *Airpower for Strategic Effect*, 34-36.
[52] This direction was a result of cooperation, more than direction. For instance, there were three separate commanders in charge of various air forces in the European Theater in 1944 – Allied Expeditionary Air Forces, RAF Bomber Command, and U.S. Strategic Air Forces in Europe. William O'Neill, *A Democracy at War*, 310.
[53] Sir Basil Liddell Hart, "The Objective in War," 18.

to the assertions of its interwar advocates, cyber power is not fated to suffer the same disappointments. With the past lessons from air power integration in mind, cyber power can also be decisive in warfare if properly applied through operational art. To that end, future doctrine should reinforce the integration of cyber operations with traditional military capabilities to ensure synergy throughout the warfighting domains.

CYBERCOM resources focused at the strategic level of war should adopt a strictly defensive mindset. General Keith Alexander, current CYBERCOM commander, is clear that his command must be prepared to defend "net users and the nation in cyberspace."[54] However, he also concedes "our adversaries in cyberspace are highly capable [but] our defenses . . . are not."[55] Thus, any strategic mindedness at CYBERCOM should first be focused on safeguarding DOD networks and securing communications in and through cyberspace.

Contrary to the assertions of current cyber power advocates, U.S. military cyber resources should not be utilized in the same manner as the "strategic bomber" assets of WWII. As Liddell Hart stated in 1952, strategic attack aimed at "direct economic and moral effect on the opposing nation, in the belief that it [will] prove more decisive, and more quickly, than cooperative action against the enemy's armed forces" proved grossly inadequate.[56] Popular will and infrastructure appear as appetizing strategic targets, but planners must be careful to not "mirror image," assuming potential adversaries are as reliant on cyberspace for civil and military functions as the U.S. Additionally, the effects of

[54] General Keith B. Alexander, "Testimony," House, *Hearing before the Committee on Armed Services Subcommittee on Emerging Threats and Capabilities on Budget Request for Information Technology and Cyber Operations Programs*, 112th Cong., 2nd sess., 2012, 57.
[55] General Keith B. Alexander, "Testimony," House, *Hearing before the Committee on Armed Services Subcommittee on Emerging Threats and Capabilities on Budget Request for U.S. Cyber Command*, 112th Cong., 1st sess., 2011, 57.
[56] Sir Basil Liddell Hart, "The Objective in War," 18.

offensive cyber operations are difficult to predict, especially the "cascading effects" into the physical domains.[57] With this in mind, it is very likely that initial strategic offensive cyber attacks will fail to deliver the results promised by current cyber power advocates.

As was the case with WWII "strategic bombing," and more recently in Operations Desert Storm (Iraq) and Allied Force (Kosovo), strategic attacks often disappoint. Throughout the initial phases of these operations, air power was used primarily to achieve strategic effects – eliminating enemy leadership and infrastructure.[58] However, given the constraints of minimizing friendly losses, avoiding civilian casualties, and appeasing alliance/coalition members, air power was ultimately too restricted to be strategically decisive.[59] These considerations will continue to be pertinent to any future military operation and must be reflected in the context of cyber operations as well.

Considering the low probability of achieving strategic results through cyber operations alone, the more appropriate approach is to focus on combined arms at the operational level of war. This approach can help planners and Joint Force Commanders (JFCs) ensure unity of effort toward common military objectives, exploiting both offensive and defensive capabilities of cyber operations. Students of operational art are taught that unity of command affords the highest degree of effectiveness in achieving unity of effort.[60] Currently, however, in order to integrate cyberspace forces and capabilities into plans and orders, a JFC must request these assets through the STRATCOM commander who may then

[57] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0*, II-1, IV-1.
[58] Joseph F. Birchmeier, *The Reliability of Warden's Theory*, 37, 38.
[59] Bruce Nardulli et al., *Disjointed War: Military Operations in Kosovo* (Santa Monica, CA: RAND Arroyo Center, 2002), 44.
[60] Unity of command is having a single commander control all forces assigned to a mission. Milan Vego, *Joint Operational Warfare*, VIII-13.

direct CYBERCOM to provide assistance.[61] As mentioned earlier, this construct is similar to how the Allied Air Forces operated in the European Theater during WWII. It requires cooperation in order to achieve unity of effort and is not as efficient as a construct that provides unity of command. The CSEs and JCCs are a good initial step to better assist the JFC in integrating both offensive and defensive cyber operations into combined arms with other joint force capabilities, but air power again provides a better framework.

Hence, like the Joint Force Air Component Commander who is responsible for all aspects of joint air operations, joint doctrine should include the option for a JFC to create a Joint Force Cyberspace Component Commander (or as in the case of space operations, a Cyberspace Coordinating Authority).[62] This commander would be responsible for integrating, deconflicting, and synchronizing all offensive and defensive cyber operations with efforts in the other domains. Just as each of the other warfighting domains can doctrinally be organized into a functional component command (FCC) or coordinating authority supporting the JFC, so should the cyberspace domain.[63] As with air power, a dedicated joint force command structure will help improve the integration of both defensive and offensive cyber operations across the spectrum of joint force capabilities – the essence of combined arms.

FINAL REMARKS (Look to the Past to Find a Way Forward)

Air power may either end war or end civilization.

- Sir Winston Churchill (1933)

---

[61] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-12* (U), IV-1 (Secret Rel USA/FVEY. Information extracted is unclassified.
[62] Jason P. Quinter, *Joint Force Command and Control of Cyber Operations* (Newport, RI: U.S. Naval War College, 2012), 13.
[63] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0,* Sect. III.

Communications theorist Marshall McLuhan postulated, "Wherever a new environment goes around an old one there is always terror."[64] Certainly, Churchill's words above were an example of how new technology can be feared and in turn over-hyped. Throughout this paper, several similarities were presented between early air power assumptions and those being proposed about cyber power. The question remains whether the zealousness of cyber power theorists and strategists will influence future cyber operations doctrine in a manner ultimately detrimental to an effective joint force.

The lessons of the past are clear. The evolution of air power provides a framework to understand how cyber operations should be organized and incorporated into current doctrine and practice. The most effective use of U.S. military cyber power is strategic defense coupled with operational level cyber operations incorporated into a combined arms approach with other joint force capabilities. If organized and synchronized properly, the result will be a more effective and efficient joint force with freedom of action throughout the war fighting domains.

[64] David Betz and Tim Stevens, *Cyberspace and the State*, 12.

BIBLIOGRAPHY

Arwood, Sam, Robert Mills and Richard Raines. “Operational Art and Strategy in Cyberspace.” *International Conference on Information Warfare and Security*, April 2010: 16-20.

Admiral, Mark A. *The Evolution of Russian Offensive Air Warfare Theory: From Deep Battle to Aerospace War.* Monterey, CA: Naval Postgraduate School, 1993.

Betz, David J., and Tim Stevens. *Cyberspace and the State.* London, UK: International Institute for Strategic Studies, 2011.

Birchmeier, Joseph F. *The Reliability of Warden's Theory on the Use of Air Power.* Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2000.

Carr, Jeffrey. *Inside Cyber Warfare.* Sebastopol, CA: O'Reilly Media, 2010.

Clausewitz, Carl von. *On War.* Edited by Michael Howard and Peter Paret. Translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1989.

Copley, Gregory R. "P3R: Projection, Protection, Policing, Resilience." *Defense and Foreign Affairs Strategic Policy* 40, no. 11/12 (2012): 2, 18-19.

Copley, Gregory R. "The Transition Beyond Strategic Nuclear War." *Defense and Foreign Affairs Strategic Policy* 40, no. 11/12 (2012): 4-6, 20.

Crowell, Richard M. "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare." Newport: Naval War College, June 2012.

Derek S. Reveron, ed. *Cyberspace and national secuity: threats, opportunities, and power in a virtual world.* Washington D.C.: Georgetown University Press, 2012.

Douhet, Giulio. *The Command of the Air.* Translated by Dino Ferrari. Washington D.C.: Air Force History and Museums Program, 1998.

Gooch, John, ed. *Airpower: Theory and Practice.* Portland, OR: Frank Cass, 1995.

Gray, Colin S. *Airpower for Strategic Effect.* Maxwell AFB, AL: Air University Press, 2012.

Inhofe, James M. "Inhofe Opening Statement at Oversight Hearing for STRATCOM, CYBERCOM ." *The Office of Senator James M. Inhofe.* March 12, 2013. http://www.inhofe.senate.gov/newsroom/press-releases/-inhofe-opening-statement-at-oversight-hearing-for-stratcom-cybercom.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, 1999.

Liddell Hart, Sir Basil Henry. "The Objective in War: National Object and Military Aim." *Naval War College Review* V, no. 4 (December 1952): 1-30.

Nardulli, Bruce, Walter L. Perry, Bruce Pirnie, John Gordon and John McGinn. *Disjointed War: Military Operations in Kosovo*. Santa Monica, CA: RAND Arroyo Center, 2002.

O'Neill, William. *A Democracy at War: America's Fight at Home and Abroad in World War II.* New York: The Free Press, 1993.

Philip S. Melinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory.* Maxwell AFB, AL: Air University Press, 1997.

Quinter, Jason P. *Joint Force Command and Control of Cyber Operations: The Joint Force Cyber Component Command*. Newport, RI: U.S. Naval War College, 2012.

Schreier, Fred. "On Cyberwarfare." *Geneva Center for the Democratic Control of Armed Forces Horizon 2015 Working Paper Series.* 2012. http://www.dcaf.ch/Publications/On-Cyberwarfare.

Sheldon, John B. "Deciphering Cyberpower: Strategic Purpose in Peace and War ." *Strategic Studies Quarterly,* Summer 2011: 95-112.

Stiennon, Richard. *Surviving Cyberwar.* Lanham, MD: Government Institutes, 2010.

The Economist, "Cyber-warfare: Hype and fear," December 8, 2012. http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may.

United States Army. *Unified Land Operations,* Army Doctrine Reference Publication (ADRP) 3-0. Washington D.C.: Headquarters Department of the Army, May 2012.

United States Congress. House. *Hearing before the Committee on Armed Services Subcommittee on Emerging Threats and Capabilities on Budget Request for U.S. Cyber Command*. 112th Cong., 1st sess., 2011.

—. *Hearing before the Committee on Armed Services Subcommittee on Emerging Threats and Capabilities on Budget Request for Information Technology and Cyber Operations Programs*. 112th Cong., 2nd sess., 2012.

United States Office of the Chairman of the Joint Chiefs of Staff. *Joint Publication 3-0 Joint Operations.* Washington D.C.: U.S. Department of Defense, 2011.

—. *Joint Publication 3-12 Cyberspace Operations* (U). Washington D.C.: U.S. Department of Defense, 2013. Secret Rel USA/FVEY. Information extracted is unclassified.

—. *Joint Publication 3-13 Information Operations.* Washington D.C.: U.S. Department of Defense, 2012.

Vego, Milan. *Joint Operational Warfare: Theory and Practice.* 2007. Newport, RI: U.S. Naval War College, reprint, 2009.